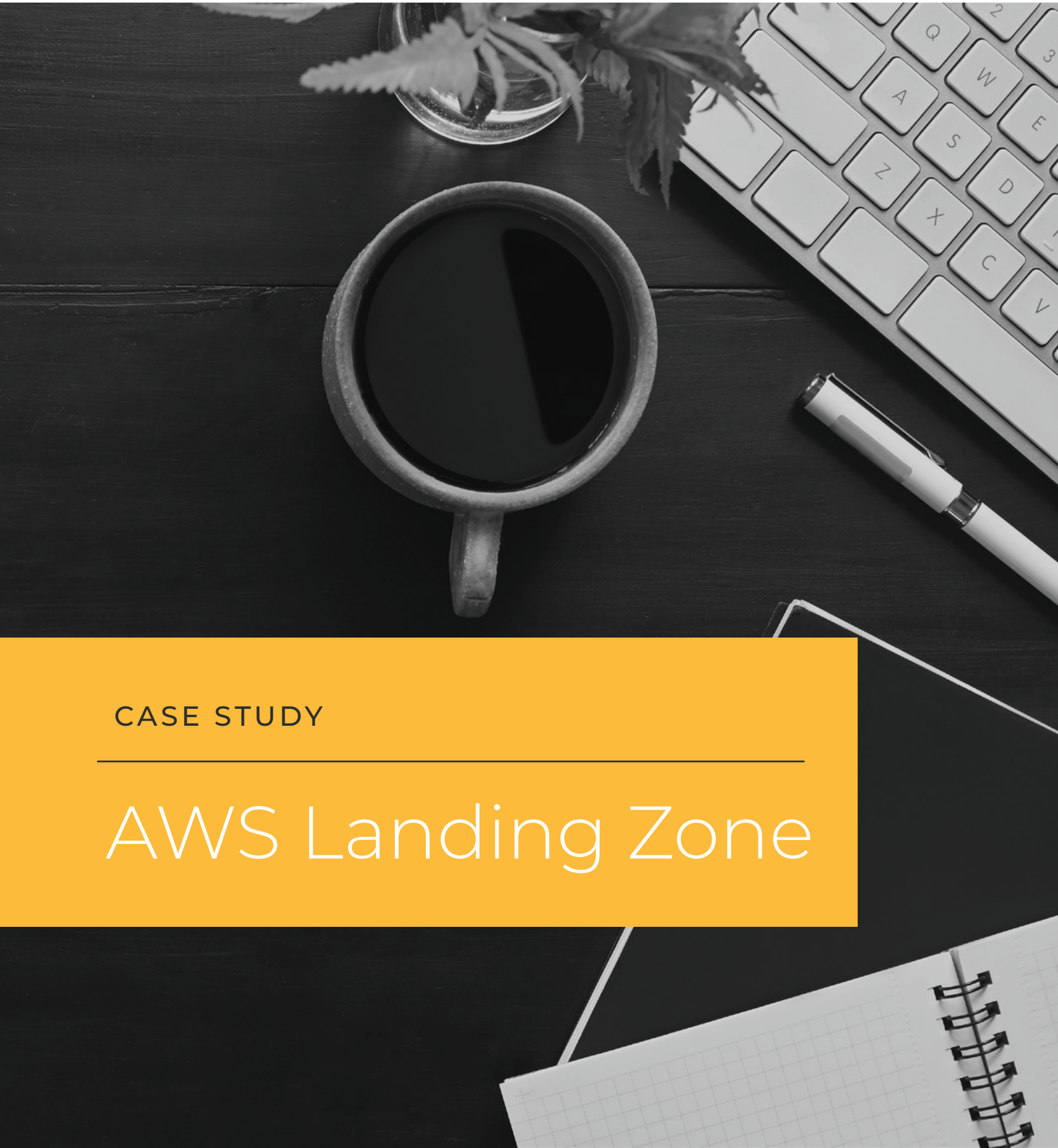
HENTSŪ
SYSTEMATIC AGILITY



CASE STUDY

AWS Landing Zone

The Challenge

In the following case study, we will be exploring how Hentsu has employed AWS (Amazon Web Services) Landing Zone as a time-saving solution to setup a reliable environment for running secure and scalable workloads.

An established firm based in the U.S. have contacted Hentsu to help them reorganize their cloud estate and supply a foundation for a much more modular and scalable infrastructure. The customer started their cloud journey just like most companies do. A single AWS account was created where people started experimenting. Not long after that, one AWS account lead to the creation of another, resources were deployed all over the place without a clear strategy or guardrails to protect the company from any potential risks.

Our customer was facing many challenges in managing their infrastructure. Some of which were:

- No clear separation between production or development resources.
- Decentralized networking with multiple exit and entry points.
- Manual deployments that are error prone and rely on key people to perform.
- Unidentifiable resources deployed in multiple regions.
- Non-existent data classification and protection.
- Hundreds of S3 buckets with inconsistent policies and encryption settings.
- Tens of IAM users with static access keys that have not been rotated for months.
- Inconsistent naming conventions.
- Non-existent billing/budgeting strategy.

It was clear to our customer that growing and sustaining their current infrastructure will be exceedingly difficult. They were looking for a ‘soft reset’ that will get them in the right shape and supply the missing foundation for their infrastructure.

Key Considerations

- The solution needs to be fully managed using code.
- The migration of the existing infrastructure should be planned, and disruptions kept to a minimum.
- Security and data protection should be high priority in the architectural design.
- The solution should be future-proof and allow for drastic changes in business needs without the need for rearchitecting.
- There should be a clear separation between development and production environments.
- Billing should be transparent and easy to understand with the ability to create custom reports based on usage, cost centre, environment, ownership, and so on.

The Solution – AWS Landing Zone

After careful examination of the needs of our customer and multiple discussion sessions we have decided to implement a Landing Zone for them. This was the perfect opportunity to use AWS Landing Zone, as a solution.

What is a Landing Zone?

A landing zone is a combination of best practices, well-designed architectural patterns and added features. The main goal for the landing zone is to bring structure, modularity and to alleviate the maintenance overhead through well-defined policies and rules. The landing zone consists of Core Accounts (Core), which act as the “control plane” of the infrastructure and Business Unit Accounts (BUs). The BUs are the pluggable accounts, which host your infrastructure resources. The goal of this separation is to is to keep your Core accounts static and allow you to add or remove BU accounts on demand without having an impact on the overall framework.

Another key part of AWS Landing Zone as a solution is the ability to centralize policies and define an overall perimeter control of the cloud organization.

INFRASTRUCTURE AS CODE

We started by deploying a brand-new landing zone for our customer. This automatically supplied the crucial foundation for a manageable infrastructure. The deployment is fully automated using Terraform and it takes less than 15 minutes. This change was also the fundamental change in our client's perspective towards infrastructure management. We have played a key role in the adoption of Terraform in their environment and helped them design deployment processes based on automated pipelines and automated orchestration using Terraform.

ACCOUNT STRUCTURE

The key in having sound infrastructure design is to make sure most of its moving parts stay decoupled. With that in mind, we have prepared an account structure that allows AWS accounts to be added or removed on demand. Our customer is now able to extend or shrink their cloud environment without having to rearchitect their core infrastructure.

SECURITY FEATURES

The landing zone is loaded with security features by default. We have deployed Service Control Policies to help us enforce protections globally. Deploying resources outside of whitelisted regions was denied, unencrypted S3 buckets or public access on buckets was denied, changes to the network infrastructure was only allowed to Network administrators etc.

We have enabled Amazon GuardDuty to supply intelligent threat detection and continuous monitoring of the environment.

AWS Security Hub was also enabled to make sure the security posture of the environment is on track with the latest security frameworks.

AWS Config and many security rules were deployed to not only alert us on unusual configuration changes but to automatically take remediation actions against these changes.

Our client is also using DarkTrace as their threat detection solution, so we have enabled that in conjunction with GuardDuty. In doing so we supplied even more comprehensive security view of the environment. More importantly, everything is powered up by sophisticated AI threat evaluation models.

AUDIT LOGS

Absolutely any action in the cloud environment is recorded and kept for a specified time. This includes AWS accounts that are active plus any accounts that have been part of the landing zone but then were terminated. The customer has decided to keep their audit logs for at least 5 years.

NETWORK CENTRALIZATION

In the pre-existing environment our customer was dealing with multiple VPCs and a full mesh of VPC peerings. The landing zone brings with itself a Transit Gateway deployment, which helps to centralize the network. We have deployed two firewalls, each in a separate availability zone for redundancy. We then changed each Transit Gateway route table to make sure any traffic leaving or coming into the environment is first evaluated by the cloud firewalls. This supplied an instant simplification of the current network setup and allowed the network team to have a complete visibility of their network perimeter.

WORKLOAD SEPARATION

It was clear that production and dev workloads were mixed up in the pre-existing environment. Anyone could just stop a production EC2 instance or delete an S3 bucket with an important data in it.

We have decided to create added AWS accounts to help isolate the current workloads in their own bubble. Development and Production resources were rehomed to their new accounts. This at once supplied access and billing separation between the two workloads. It was now clear to the accounts team how much development and research is costing vs production. It is not possible to accidentally shutdown or delete production resources anymore as the access needed for the production account is different compared to development.

DATA PROTECTION

We have employed the use of KMS keys to ensure that all data at rest is encrypted. Data in transit, even within the VPC was also encrypted using technologies like TLS. Unencrypted and unprotected resources are automatically flagged by AWS Config making it impossible for the cloud environment to stay out of compliance without people being notified about it.

CONSISTENCY

In the pre-existing environment we had resources either using different naming conventions, tags or not having any tags at all. Through the Security Control Policies and Tag Policies that AWS Organizations provide, we were able to define and enforce a tagging/naming strategy. It is no longer possible to create resources without following the global tagging policy.

COST CONTROL AND BILLING

The combination of a solid tagging strategy, billing consolidation and good account structure allows for much granular and flexible cost reports to be generated. Spending additional sessions with the accounts team helped us better understand what billing reports will supply most value to them. We then enabled additional cost categories and cost allocation tags to match their requirements.

Both soft and hard budgets were created to ensure unexpected costs are under control. Hard stop budgets were carefully designed to stop only resources that are not business critical (e.g. development instances). As another cost optimization strategy, we have bought Savings Plans for the core compute resources with the choice to expand the reservation based on the long-term business plans.

Impact

This project allowed us to reap the benefits of AWS Landing Zone. The radical change from having multiple standalone AWS accounts to using a Landing Zone with clearly defined control plane, security policies and centralized management have allowed our client to better focus on their present and future tasks without worrying the infrastructure will support it.

The development team was able to self-serve their way in the unique environment without having to worry about performing breaking network changes or accidentally removing production resources. This additionally increased the speed of developing, testing, and releasing new features.

The customer started their journey towards managing infrastructure using code and happily adopted the Git workflows we have designed for them. It is now easy for them to peer review changes, roll back and supply a history of all changes ever made in the environment using their CI/CD platform.

It is no longer a mystery to find who is the owner of a given resource. The naming conventions and tag policies have allowed for the creation of a truly consistent and self-describing infrastructure, making it easy even for new joiners to navigate around.

HENTSŪ LONDON

30 Crown Place
London, EC2A 4EB
United Kingdom
+44 203 857 1630

HENTSŪ NEW YORK

600 Fifth Avenue
New York, NY 10020
United States
+1 315 257 4284

HENTSŪ BOSTON

125 High Street
Boston, MA 02110
United States
+1 315 257 4284